NETCheck

Política de seguridad de la información ENS

CONTROL DE REVISIONES		
FECHA REVISIÓN	N.º DE REVISIÓN	OBSERVACIONES
10/10/2020	1.0	Primera versión
07/12/2022	2.0	Segunda versión
05/11/2024	3.0	Actualización de requisitos legales

Índice

1. APROBACIÓN Y ENTRADA EN VIGOR 3
2. ALCANCE 3
3. OBJETIVOS 3
4. MARCO NORMATIVO 4
5. DESARROLLO 4
6. ORGANIZACIÓN DE LA SEGURIDAD 5
7. COMITÉ DE SEGURIDAD 6
8. GESTIÓN DE RIESGOS 6
9. GESTION DE PERSONAL 7
10. PROFESIONALIDAD Y SEGURIDAD DE LOS RECURSOS HUMANOS 7
11. CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN 9
12. PROTECCIÓN DE LAS INSTALACIONES 9
13. ADQUISICIÓN DE PRODUCTOS 10
14. SEGURIDAD POR DEFECTO 10
15. INTEGRIDAD Y ACTUALIZACION POR DEFECTO 11
16. PROTECCION DE LA INFORMACION ALMACENADA Y EN TRANSITO 11
17. PREVENCION DE SISTEMAS DE INFORMACION INTERCONECTADOS 11
18. REGISTROS DE ACTIVIDAD 12
19. CONTINUIDAD DE LA ACTIVIDAD 12
20. MEJORA CONTINUA EN LOS PROCESOS DE SEGURIDAD 13

1. APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información es efectiva desde la fecha de firma y hasta que sea reemplazada por una nueva Política.

2. ALCANCE

Esta política se aplica a todos los sistemas TIC de la entidad y a todos los miembros de la organización, implicados en Servicios y Proyectos destinados al sector público, que requieran la aplicación de ENS, sin excepciones.

3. OBJETIVOS

NETCheck es una empresa especializada en consultoría y soluciones tecnológicas con un amplio abanico de posibilidades según las necesidades de nuestros clientes. Desde cómo gestionar el departamento de compras a ODT en la administración pública. Ayudamos a empresas en la gestión de cambios tecnológicos y proyectos, ofreciendo soluciones tecnológicas con diversas prestaciones IT en el sector público.

Nuestros compromisos en seguridad de la información son:

- Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz.
- Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones
- Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información

Para poder lograr estos objetivos es necesario:

- Mejorar continuamente nuestro sistema de seguridad de la información
- Cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribamos además de los compromisos adquiridos con los clientes, así como la actualización continúa de los mismos.

4. MARCO NORMATIVO

El marco legal y regulatorio en el que desarrollamos nuestras actividades es:

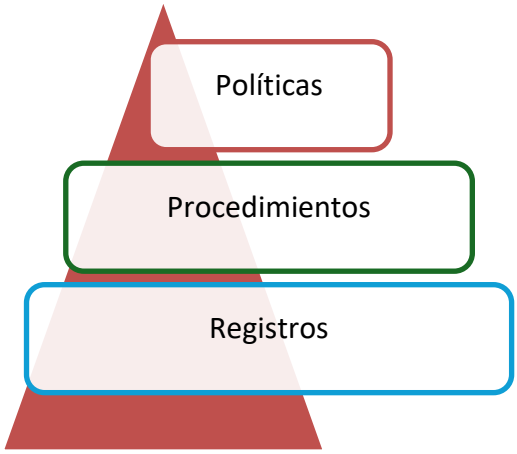
- **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016** relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- **Ley Orgánica 3/2018, de 5 de diciembre**, de Protección de Datos Personales y
- Garantía de los derechos digitales (LOPD)
- **Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual**
- **Real Decreto-ley 2/2018, de 13 de abril**, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual
- **Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad**
- **Ley 34/2002 de 11 de Julio de Servicios de la sociedad de la Información y de Comercio Electrónico (LSSI)**

5. DESARROLLO

Para poder lograr todos los objetivos, es necesario:

- Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, caso de materializarse, puedan causar.
- Preservar los intereses de sus principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.
- Trabajar de forma conjunta con nuestros suministradores y subcontratistas con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, que repercutan en una mayor eficiencia de nuestra actividad.
- Evaluar y garantizar la competencia técnica del personal, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.
- Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.

- Garantizar un análisis de manera continua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- Estructurar nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión tiene la siguiente estructura:



La gestión de nuestro sistema se encomienda al responsable de Gestión y el sistema estará disponible en nuestro sistema de información en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos.

6. ORGANIZACIÓN DE LA SEGURIDAD

Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de la presente Política Integrada de Sistemas de Gestión.

Los roles o funciones de seguridad definidos en **NETCHECK** son:

Función	Deberes y responsabilidades
Responsable de la información	❑ Tomar las decisiones relativas a la información tratada
Responsable de los servicios	❑ Coordinar la implantación del sistema ❑ Mejorar el sistema de forma continua
Responsable de la seguridad	❑ Determinar la idoneidad de las medidas técnicas ❑ Proporcionar la mejor tecnología para el servicio

Responsable del sistema	❑ Coordinar la implantación del sistema ❑ Mejorar el sistema de forma continua
Dirección	❑ Proporcionar los recursos necesarios para el sistema ❑ Liderar el sistema

Esta definición se completa en los perfiles de puesto y en los documentos del sistema.

7. COMITÉ DE SEGURIDAD

El procedimiento para su designación y renovación será la ratificación en el comité de seguridad

El comité para la gestión y coordinación de la seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité. Los miembros del comité de seguridad de la información son:

- Responsable de la información.
- Responsable de los servicios.
- Responsable de la seguridad.
- Responsable del sistema.
- Dirección Empresa.

Estos miembros son designados por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos.

El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de **NETCHECK**

Está política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión.

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se revisa regularmente:

- Al menos una vez al año;
- Cuando cambie la información manejada;

- Cuando cambien los servicios prestados;
- Cuando ocurra un incidente grave de seguridad;
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Para la realización del análisis de riesgos se tendrá en cuenta la metodología de análisis de riesgos desarrollada en el procedimiento Análisis de Riesgos.

9. GESTION DE PERSONAL

Todos los miembros de **NETCHECK** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **NETCHECK** atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **NETCHECK**, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

10. PROFESIONALIDAD Y SEGURIDAD DE LOS RECURSOS HUMANOS

Esta Política se aplica a todo el personal de **NETCHECK** y el personal externo que realiza tareas dentro de la empresa.

RRHH incluirá funciones de seguridad de la información en las descripciones de los trabajos de los empleados, informará a todo el personal que contrate sus obligaciones con respecto al cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de los usuarios con respecto a esta Política.

- El responsable de la seguridad, es responsable de monitorear, documentar y analizar los incidentes de seguridad reportados, así como de comunicarse al Comité de Seguridad de la Información y a los propietarios de información.
- El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el responsable de la Seguridad maneje informes de incidentes y anomalías del sistema. El Comité también estará al tanto, supervisará la investigación, supervisará la evolución de la información y promoverá la resolución de incidentes de seguridad de la información.
- El responsable de Gestión de la Seguridad (RGS) [CISO] participará en la preparación del Compromiso de Confidencialidad que firmará los empleados y terceros que desempeñen funciones en **NETCHECK** en el asesoramiento sobre las sanciones que se aplicarán por incumplimiento de esta Política y en el tratamiento de incidentes de seguridad de la información.
- Todo el personal de **NETCHECK** es responsable de informar sobre las debilidades e incidentes de seguridad de la información que se detectan oportunamente.
- Profesionalidad de los recursos humanos:
- Determinar la competencia necesaria del personal para llevar a cabo el trabajo que afecta a la Seguridad de la Información.
- Hay que asegurar que las personas sean competentes sobre la base de la educación, capacitación o experiencia adecuadas.
- Demostrar mediante la información documentada que sea necesaria la competencia del personal en materia de Seguridad de la Información.

Los objetivos de controlar la seguridad del personal son:

- Reducir los riesgos de error humano, puesta en marcha de irregularidades, uso indebido de instalaciones y recursos, y manejo no autorizado de la información.
- Explicar las responsabilidades de seguridad en la etapa de reclutamiento del personal e incluirlas en los acuerdos a firmar y verificar su cumplimiento durante el desempeño de las tareas del empleado.
- Asegúrese de que los usuarios estén al tanto de las amenazas y preocupaciones de seguridad de la información y estén capacitados para apoyar la Política de Seguridad de la Información de la organización en el curso de sus tareas normales.
- Establecer compromisos de confidencialidad con todo el personal y usuarios fuera de las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de las debilidades de seguridad existentes, así como los incidentes, con el fin de minimizar sus efectos y prevenir su reincidencia.

11. CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

El control del acceso a los sistemas de información tiene por objetivo:

- Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.
- Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de **NETCHECK** y otras redes públicas o privadas.
- Revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.
- Concienciar sobre su responsabilidad por el uso de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y ordenadores personales para el trabajo remoto.

12. PROTECCIÓN DE LAS INSTALACIONES

Los objetivos de esta política en materia de protección de las instalaciones son:

- Prevenir el acceso no autorizado, daños e interferencias a la sede, instalaciones e información de **NETCHECK**
- Proteger el equipo de procesamiento de información crítico de **NETCHECK** colocándolo en áreas protegidas y protegido por un perímetro de seguridad definido, con las medidas de seguridad y controles de acceso adecuados. Asimismo, contemplar la protección de esta en su traslado y permanecer fuera de las áreas protegidas, por mantenimiento u otros motivos.
- Controlar los factores ambientales que podrían perjudicar el buen funcionamiento del equipo de cómputo que alberga la información de **NETCHECK**
- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus tareas habituales.
- Proporcionar protección proporcional a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relacionados con los sistemas de información de **NETCHECK**: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.

El responsable de Gestión de la Seguridad, junto con los Titulares de la Información, según proceda, definirá las medidas de seguridad física y ambiental para la protección de los activos críticos, sobre la base de un análisis de riesgos, y supervisará su aplicación. También verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.

Los responsables de los diferentes departamentos definirán los niveles de acceso físico del personal de **NETCHECK** a las áreas restringidas bajo su responsabilidad. Los Propietarios de Información autorizará formalmente el trabajo fuera del sitio con información sobre su negocio a los empleados de **NETCHECK** cuando lo consideren apropiado.

Todo el personal de **NETCHECK** es responsable del cumplimiento de la política de pantalla limpia y escritorio, para la protección de la información relacionada con el trabajo diario en las oficinas.

13. ADQUISICIÓN DE PRODUCTOS

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por otro lado, se tendrá en cuenta la seguridad de la información en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.

La política de desarrollo y adquisición de sistemas de información se desarrolla en el documento: Política Adquisición, Desarrollo y Mantenimiento de Sistemas.

14. SEGURIDAD POR DEFECTO

NETCHECK considera estratégico para la entidad que los procesos integren la seguridad de la información como parte de su ciclo de vida. Los sistemas de información y los servicios deben incluir la seguridad por defecto desde su creación hasta su retirada, incluyéndose la seguridad en las decisiones de desarrollo y/o adquisición y en todas las actividades en explotación estableciéndose la seguridad como un proceso integral y transversal.

15. INTEGRIDAD Y ACTUALIZACION POR DEFECTO

NETCHECK se compromete a garantizar la integridad del sistema mediante un proceso de gestión de cambios que permita el control de la actualización de los elementos físicos o lógicos mediante la autorización previa a su instalación en el sistema. Dicha evaluación será llevada a cabo principalmente por la dirección de sistemas que evaluará el impacto en la seguridad del sistema antes de realizar los cambios y controlará de forma documentada aquellos cambios que se evalúen como importantes o con implicaciones en la seguridad de los sistemas.

Mediante revisiones periódicas de seguridad se evaluará el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

16. PROTECCION DE LA INFORMACION ALMACENADA Y EN TRANSITO

NETCHECK establece medidas de protección para la Seguridad de la Información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

17. PREVENCION DE SISTEMAS DE INFORMACION INTERCONECTADOS

NETCHECK establece medidas de protección para la Seguridad de la Información especialmente para proteger el perímetro, en particular, si se conecta a redes públicas, especialmente si se utilizan en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público.

En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión. Conexiones electrónicas disponibles para el público.

18. REGISTROS DE ACTIVIDAD

NETCHECK registrará las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Los objetivos principales de la Gestión de incidentes son los de:

- Establecer un sistema de detección y reacción frente a código dañino
- Disponer de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.
- Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones.
- Este registro se emplea para la mejora continua de la seguridad del sistema.
- Garantizar que los servicios de IT vuelvan a tener un desempeño óptimo.
- Reducir los posibles riesgos e impactos que pueda causar el incidente.
- Velar por la integridad de los sistemas en el caso de un incidente de seguridad.
- Comunicar el impacto de un incidente tan pronto como se detecte para activar la alarma; y poner en práctica un plan de comunicación empresarial adecuado.
- Promover la eficiencia empresarial.

19. CONTINUIDAD DE LA ACTIVIDAD

NETCHECK con el objetivo de garantizar la continuidad de las actividades, establece medidas para que los sistemas dispongan de copias de seguridad y establece mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

20. MEJORA CONTINUA EN LOS PROCESOS DE SEGURIDAD

NETCHECK establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida en normas internacionales como ISO 27001.